CA Nimsoft Monitor Server

Notas da Versão e Guia de Atualização

7.0

Histórico da revisão do documento

Versão do NMS	Data	Alterações
7.00	Setembro de 2013	Revisões para o NMS v7.00
6.50	Março de 2013	Revisões do NMS v6.50
6.20	Dezembro de 2012	Revisões do NMS v6.20
6.10	Setembro de 2012	Atualizado e revisado para o NMS v6.10
6.00	Junho de 2012	Revisões do NMS v6.00
5.61	Abril de 2012	Observação sobre scripts de atualização grandes do banco de dados MySQL
5.61	Março de 2012	Atualizações na documentação
5.61	Fevereiro de 2012	Correções e atualizações na documentação
5.61	Janeiro de 2012	Revisões para o NMS v5.61
5.60	Dezembro de 2011	Revisões do NMS v5.60

Avisos legais

Garantia

O material contido neste documento é fornecido "como está" e está sujeito a alterações em edições futuras sem aviso prévio. Além disso, na medida permitida pela lei aplicável, a Nimsoft LLC isenta-se de todas as garantias, sejam implícitas ou expressas, com relação a este manual e todas as informações contidas no presente documento, incluindo, sem limitação, garantias implícitas de comerciabilidade e adequação para um determinado fim. A Nimsoft LLC não será responsabilizada por erros ou danos acidentais ou resultantes do fornecimento, uso ou desempenho deste documento ou de qualquer outra informação contida no presente. Caso a Nimsoft LLC e o usuário tenham um acordo por escrito à parte sobre termos de garantia que cobrem o material deste documento conflitando com estes termos, os termos de garantia do acordo à parte prevalecerão.

Licenças de tecnologia

O hardware e/ou software descritos neste documento são fornecidos sob uma licença e poderão ser usados ou copiados somente de acordo com os termos da referida licença.

Nenhuma parte deste manual poderá ser reproduzida de qualquer forma ou por qualquer meio (incluindo a recuperação e o armazenamento eletrônico ou a tradução em um idioma estrangeiro) sem um acordo prévio e consentimento por escrito da Nimsoft LLC, em conformidade com as leis de direitos autorais internacional e dos EUA.

Legenda de direitos restritos

Se o uso do software for destinado ao cumprimento de um contrato ou subcontrato do governo dos Estados Unidos da América -EUA, o software será fornecido e licenciado como "software comercial para computadores", conforme definido no DFAR 252.227-7014 (junho de 1995), ou como um "item comercial", conforme definido no FAR 2.101(a); ou como "software de computador restrito", conforme definido no FAR 52.227-19 (junho de 1987) ou em qualquer regulamento equivalente do órgão ou Cláusula contratual. O uso, a duplicação ou a divulgação do software está sujeito aos termos de licença comercial padrão da Nimsoft LLC, os departamentos que não fazem parte do DOD (Department of Defense) e os órgãos do governo dos EUA não receberão mais Direitos do que os Direitos Restritos, conforme definido no FAR 52.227-19(c)(1-2) (junho de 1987). Os usuários do governo dos EUA não receberão mais que Direitos Limitados, conforme definido no FAR 52.227-14 (junho de 1987) ou no DFAR 252.227-7015 (b)(2) (novembro de 1995), conforme aplicável em quaisquer dados técnicos.

Marcas registradas

Nimsoft é uma marca registrada da CA.

Adobe®, Acrobat®, Acrobat Reader® e Acrobat Exchange® são marcas registradas da Adobe Systems Incorporated.

Intel® e Pentium® são marcas registradas da Intel Corporation dos EUA.

Java(TM) é uma marca registrada da Sun Microsystems, Inc. dos EUA.

Microsoft® e Windows® são marcas registradas da Microsoft Corporation dos EUA.

Netscape(TM) é uma marca registrada da Netscape Communications Corporation dos EUA.

Oracle® é uma marca registrada da Oracle Corporation, Redwood City, Califórnia, Estados Unidos.

UNIX® é uma marca registrada do Open Group.

ITIL® é uma marca comercial registrada do Office of Government Commerce no Reino Unido e em outros países.

Todas as marcas comerciais, nomes comerciais, marcas de serviços e logotipos mencionados neste documento pertencem às respectivas empresas.

Para obter informações sobre software de domínio público e licença, consulte a *Licença de Terceiros e Termos de Uso do Nimsoft Monitor* do documento no site: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Entre em contato com a CA Nimsoft

Entrar em contato com a CA Support

Para sua conveniência, a CA Technologies oferece um site onde é possível acessar as informações necessárias a seus produtos da CA Technologies para escritório doméstico, pequena empresa e corporativos. Em http://www.ca.com/worldwide, é possível acessar os seguintes recursos:

- Informações para contato online e telefônico, assistência técnica e atendimento ao cliente
- Informações sobre fóruns e comunidades de usuário
- Downloads de produto e documentação
- Políticas e diretrizes de CA Support
- Outros recursos úteis adequados ao seu produto

Fornecendo comentários sobre a documentação do produto

Enviar comentários ou perguntas sobre a documentação de produtos da Nimsoft da CA Technologies para nimsoft.techpubs @ ca.com.

Se desejar fornecer comentários sobre a documentação geral dos produtos da CA Technologies, responda nossa breve pesquisa do cliente, disponível no site de CA Support, encontrado em http://ca.com/docs.

Índice

Capítulo 1: Funcionalidades novas e alteradas

O Nimsoft Monitor Server (NMS) 7.00 é uma release principal que melhora a estabilidade, a escalabilidade, o desempenho, os recursos e a funcionalidade do produto, adicionando estes novos recursos importantes:

- Monitoramento de rede aprimorado (Coletor SNMP).
- Melhoria do programa de instalação.
- Melhoria da detecção automatizada com a correlação de dispositivos aprimorada.
- Melhoria do desempenho da escalabilidade do barramento de mensagens (hub 7.0)
- Aplicativo móvel 7.0.
- O Console de administração se comunica com o NMS usando HTTP pela porta 8080 por padrão. A comunicação segura usando HTTPS pela porta 8443 é uma opção.
- O processo de configuração de certificados autoassinados foi simplificado; sendo a segurança de 2048 bits a configuração padrão.
- O Unified Reporter atualizado restaura o suporte a dados em séries de temporizador nos relatórios ad hoc
- Monitoramento de armazenamento expandido (Hitachi AMS e HUS).

Alterações de componente

- Melhoria do desempenho e da estabilidade do hub.
- O probe service_host pode anunciar a si próprio como um serviço para outros componentes da Nimsoft usando um endereço IP ou um nome de host.
- O probe vmware publica dados de detecção para a detecção automatizada.
- Gerenciador de NiS removido do NMS 7.0.
- A funcionalidade de script LUA usada para processar os resultados do discovery_agent foi removida.
- A Detecção de serviço foi removida do discovery_server e do discovery_agent.

Capítulo 2: Requisitos

Sistemas com suporte

Observação: com a versão 6.50 e posteriores, o servidor do Nimsoft Monitor só pode ser instalado nas versões de *64 bits* dos sistemas operacionais suportados. Os detalhes sobre a migração de uma instalação existente do NMS de um sistema de 32 bits para um sistema de 64 bits não são abordados neste guia, entre em contato com o suporte da Nimsoft http://support.nimsoft.com.

Para disponibilizar as informações mais recentes, os requisitos de sistema para o NMS são fornecidos no site de suporte da Nimsoft, support.nimsoft.com http://support.nimsoft.com.

- Para obter uma lista de sistemas operacionais, bancos de dados, navegadores e versões JRE com suporte, consulte a Matriz de suporte de compatibilidade da Nimsoft.
- Para obter informações sobre os componentes que estão sendo substituídos ou que não têm mais suporte, consulte a parte final do documento de venda da Nimsoft:

  http://support.nimsoft.com/Files/Announcement/current_-_end_of_sales_announcement.pdf

Componente Infraestrutura do Nimsoft

A Infraestrutura do Nimsoft faz parte da instalação do servidor do Nimsoft. Se desejar instalar apenas a Infraestrutura do Nimsoft (hubs, robôs ou probes) em um sistema UNIX® adicional, os sistemas UNIX® a seguir têm suporte:

- AIX
- HP-UX
- Linux
- Solaris

Mais informações também estão disponíveis online, na Matriz de suporte de compatibilidade da Nimsoft, que é atualizada regularmente.

Requisitos do sistema adicionais

- O Mecanismo de dados requer libstdc++.so.5 { libstdc++-3.3.4-11.x86_64.rpm } em distribuições do OpenSUSE Linux
- O banco de dados *não* deve diferenciar maiúsculas de minúsculas ao controlar as consultas.
- A verificação de espaço livre do banco de dados não está implementada para Oracle e MySQL.

Idiomas com suporte

O CA Nimsoft Monitor Server está disponível nestes idiomas:

- Inglês
- Chinês simplificado
- Japonês
- Espanhol
- Português do Brasil

Capítulo 3: Considerações

Esta seção descreve as características encontradas nesta release que afetam a versão 7.0 da instalação, da atualização, da localização ou do comportamento em geral do NMS.

Dimensionamento do sistema

Para obter as informações mais recentes sobre dimensionamento, consulte a seção Recomendações de hardware, no *Guia de Instalação do Servidor do NMS*, disponível na página de download no suporte da Nimsoft http://support.nimsoft.com.

Programas de instalação

O programa de instalação do NMS oferece as seguintes opções de instalação:

- Uma **GUI** (Graphical User Interface - Interface Gráfica do Usuário) nos sistemas Windows, Linux e Solaris.
- **Modo de console** nos sistemas Linux e Solaris.
- **Modo silencioso** nos sistemas Windows, Linux e Solaris (você especifica os valores do parâmetro de instalação em um arquivo que é usado para concluir a instalação sem interação com o usuário).

Para obter mais detalhes, consulte a seção sobre Instalação do servidor no *Guia de Instalação do NMS*, também disponível na página de download de suporte da Nimsoft http://support.nimsoft.com.

Privilégios de logon necessários

Use um logon com privilégios de administrador (Windows) ou de raiz (UNIX®) ao instalar ou atualizar para o NMS 7.0. Observe que se o banco de dados for:

- **Criado antes da instalação do NMS**, o logon usado durante a instalação ou atualização deve mapear para as credenciais válidas do DBA do banco de dados.
- **Criado pelo programa de instalação do NMS**, as credenciais do banco de dados resultantes serão automaticamente mapeadas para o logon usado durante a instalação.

Instalar dois ou mais hubs

A Nimsoft recomenda que você instale pelo menos dois hubs do Nimsoft no mesmo domínio e rede para evitar perda de dados de usuário/segurança (Definições de usuário Nimsoft, ACLs, etc.) no caso de falha do sistema do hub principal. Com mais de um hub, essas informações são espelhadas entre os hubs.

Desative o qos_processor antes de instalar o UMP

Ao instalar ou atualizar o UMP com o MySQL, desative o probe qos_processor antes de executar o programa de instalação do UMP. Quando o UMP estiver instalado, o processador de QoS poderá ser reativado.

Após atualizar o NMS**:**

> Com base no uso do Console de administração ou no Gerenciador de infraestrutura, CA Nimsoft recomenda *fazer download da versão mais recente do probe ppm* (gerenciador de provisionamento do probe) a partir do arquivo do probe localizado no site de suporte da CA Nimsoft (support.nimsoft.com). A atualização do sistema para o probe ppm mais recente garante que você tenha acesso à funcionalidade mais recente do Console de administração.

Capítulo 4: Atualizando o servidor do Nimsoft

Esta seção explica como atualizar para o NMS 7.0.

Esse processo consiste em uma cadeia de atualizações para os módulos instalados no momento. **NÃO** reinicie o sistema até que todos os módulos tenham sido instalados, até mesmo se receber solicitações do sistema para reiniciar em pontos intermediários do processo.

Antes de atualizar

Os programas de instalação do NMS (GUI, console e silencioso) permitem atualizar o NMS facilmente. Ao atualizar, sua configuração (nomes de domínio e hub, endereços IP, contas de usuário, senhas, etc.) é mantida.

Antes de executar o programa de instalação:

- **Desative o encaminhamento de pacotes e limpe a fila de tarefas do distsrv.**

  O encaminhamento de pacotes está configurado na GUI do probe distsrv. Para exibir a fila, selecione Tools > Distribution no Infrastructure Manager. A atualização falhará se a fila de tarefas do distsrv tiver tarefas pendentes. Após uma atualização bem-sucedida, reative o encaminhamento de pacotes no distsrv, se desejar.

- **Remova os probes personalizados do arquivo morto de probes (recomendado).**

  Mova ou exclua os probes personalizados do arquivo morto de probes; mantenha os probes básicos de infraestrutura. Após a conclusão de todas as instalações e atualizações (principalmente para UMP e Unified Reporter), você pode mover os probes seletivamente de volta para o arquivo morto.

- **Fazer backup da configuração do hub (recomendável)**

  Salvar uma cópia do arquivo hub.cfg na pasta Nimsoft\hub. Os parâmetros ideais de tempo limite para o hub atualizado são definidos durante a atualização, substituindo configurações de tempo limite existentes. A Nimsoft recomenda executar o hub atualizado com estes valores ideais para obter um desempenho aprimorado. No entanto, se você deseja reverter para as configurações antigas de tempo limite por qualquer motivo, mantenha um backup do antigo arquivo de configuração do hub.

Você deve atualizar o NMS antes de atualizar o UMP. Isso garantirá que o esquema de banco de dados necessário do qual o UMP depende esteja operacional.

Para encontrar os caminhos de atualização com suporte, consulte a matriz de suporte de compatibilidade no site de suporte da Nimsoft.

Atualizando o sistema do NMS

Atualizando o NMS no Windows — Modo GUI

Quando você atualiza o sistema do NMS, a configuração existente é mantida, tornando uma atualização muito mais simples do que uma nova instalação.

Importante: todos os campos das caixas de diálogo do programa de instalação diferenciam maiúsculas de minúsculas.

1. Desative os programas antivírus em execução no servidor (esses programas podem diminuir a velocidade de instalação de forma significativa).

   Observação: ative os programas antivírus imediatamente após a instalação.

2. Verifique se você desativou o encaminhamento de pacotes, limpou a fila de tarefas do distsrv (necessário) e removeu os probes personalizados do arquivo morto de probes (recomendado).
3. Efetue logon no site de Atendimento ao cliente da Nimsoft http://support.nimsoft.com.
4. Faça download e execute o pacote de instalação mais recente do NMS para Windows.
5. Siga os prompts para concluir a instalação. Sempre que possível, o programa de instalação exibe os valores de configuração atuais para sua confirmação.
6. Quando a atualização estiver concluída, certifique-se de:
   - Ativar os programas antivírus novamente, se necessário.
   - Ativar o encaminhamento de pacotes.
   - Mover os probes personalizados de volta para o arquivo morto de probes, se necessário.
   - Atualizar os componentes (hubs, robôs, consoles de gerenciamento, etc.) na implantação do Nimsoft.

Atualizando o NMS em Linux ou Solaris — Modo de console

Quando você atualiza o sistema do NMS, a configuração existente é mantida, tornando uma atualização muito mais simples do que uma nova instalação.

Siga estas etapas:

1. Desative os programas antivírus em execução no servidor (esses programas podem diminuir a velocidade de instalação de forma significativa).

   Observação: ative os programas antivírus imediatamente após a instalação.

2. Verifique se você desativou o encaminhamento de pacotes, limpou a fila de tarefas do distsrv (necessário) e removeu os probes personalizados do arquivo morto de probes (recomendado).
3. Efetue logon no site de Atendimento ao cliente da Nimsoft http://support.nimsoft.com.
4. Faça download e execute o pacote de instalação mais recente do NMS para Linux ou Solaris (o pacote tem mais de 1 GB, portanto, essa operação pode levar vários minutos).
5. Execute **chmod 755** no arquivo de instalação para torná-lo executável.
6. Execute o programa de instalação. Em uma linha de comando, execute:
   - Linux: **installNMS_linux.bin -i console**
   - Solaris: **installNMS_solaris.bin -i console**
7. Siga os prompts para concluir a instalação. Sempre que possível, o programa de instalação exibe os valores de configuração atuais para sua confirmação.
8. Quando a atualização estiver concluída, certifique-se de:
   - Ativar os programas antivírus novamente, se necessário.
   - Ativar o encaminhamento de pacotes.
   - Mover os probes personalizados de volta para o arquivo morto de probes, se necessário.
   - Atualizar os componentes (hubs, robôs, consoles de gerenciamento, etc.) na implantação do Nimsoft.

Atualizando o NMS no Windows, Linux ou Solaris — Modo silencioso

Quando você atualiza o sistema do NMS, a configuração existente é mantida, tornando uma atualização muito mais simples do que uma nova instalação.

Siga estas etapas:

1. Desative os programas antivírus em execução no servidor (esses programas podem diminuir a velocidade de instalação de forma significativa).

   Observação: ative os programas antivírus imediatamente após a instalação.

2. Verifique se você desativou o encaminhamento de pacotes, limpou a fila de tarefas do distsrv (necessário) e removeu os probes personalizados do arquivo morto de probes (recomendado).
3. Efetue logon no site de Atendimento ao cliente da Nimsoft http://support.nimsoft.com.
4. Faça download:
   - Do pacote de instalação mais recente do NMS para seu sistema operacional e arquitetura.
   - Pacote de instalação silenciosa (arquivo .zip)
5. No Linux ou Solaris, execute **chmod 755** no arquivo de instalação para torná-lo executável.
6. Prepare seu arquivo de resposta:

   a. Extraia os modelos de instalação silenciosa.

   b. Localize o arquivo **installer.upgrade.properties** e salve-o como **installer.properties** no mesmo diretório que o programa de instalação.

   c. Adicione sua senha de administrador do NMS à linha **NMS_PASSWORD=** de **installer.properties**.

   d. Salve o arquivo, garantindo que o tipo de arquivo ainda é **PROPERTIES**. Se o tipo de arquivo for **Text Document**, remova a extensão **.txt** (que pode não ser exibida na pasta).

7. Execute o programa de instalação. Em uma linha de comando, execute:
   - Windows: **installNMS.exe -i silent**
   - Linux: **installNMS_linux.bin -i silent**
   - Solaris: **installNMS_solaris.bin -i silent**
8. O programa de instalação descompacta os arquivos e conclui a instalação. Esse processo pode levar vários minutos ou mais. Para ver o andamento da instalação, execute:
   ```
   tail -f /tmp/ia/iaoutput.txt
   ```
9. O NMS é iniciado. Se por algum motivo não for iniciado, execute:
   - Windows: **net start Nimsoft Robot Watcher**
   - Linux ou Solaris: **cd /etc/init.**d, em seguida, **nimbus start (**ou **/etc/init.d/nimbus start**)
10. Quando a atualização estiver concluída, certifique-se de:
    - Ativar os programas antivírus novamente, se necessário.
    - Ativar o encaminhamento de pacotes.
    - Mover os probes personalizados de volta para o arquivo morto de probes, se necessário.
    - Atualizar os componentes (hubs, robôs, consoles de gerenciamento, etc.) na implantação do Nimsoft.

Atualizando o NMS em um agrupamento do MS Server

Em um agrupamento de tolerância a falhas do MS Server 2003/2008/2008 R2:

1. Atualize o NMS no nó principal (ativo), usando um dos procedimentos de atualização do Windows. Consulte:
   - Atualizando o NMS no Windows com a GUI do assistente de instalação (na página 15)
   - Atualizando o NMS no Windows, Linux ou Solaris com o modo silencioso (na página 17)
2. Torne ativo o nó secundário (passivo) e, em seguida, atualize o NMS usando o mesmo processo usado no nó principal.

Isso garante que as chaves de registro nos nós principal (ativo) e secundário (passivo) estão atualizados para a nova versão.

Atualizando os clientes do NMS

Atualizar o Infrastructure Manager

Em todos os servidores e estações de trabalho que têm o Infrastructure Manager instalado (verifique em **Iniciar > Todos os Programas > Nimsoft Monitoring**), você deve fazer a atualização para a versão mais nova.

1. Abra um navegador da web no computador em que deseja atualizar o Gerenciador de infraestrutura e acesse o Nimsoft Monitor Server na página da web no URL: <servername_or_server_IP_address>:8080.
2. Na página web exibida, escolha o link **Legacy Infrastructure Manager** para instalar a nova versão nesse computador.
3. Repita esse procedimento para atualizar outros computadores.

Observação: o **Console de administração do Nimsoft Monitor** é um novo console de gerenciamento que oferece uma alternativa independente da plataforma para o Gerenciador de infraestrutura. Ele pode ser iniciado de forma autônoma em um navegador usando o link fornecido anteriormente para a instalação do **Gerenciador de infraestrutura herdado**. Como alternativa, ele pode ser instalado como um portlet em execução no UMP.

Atualizar hubs

1. Identifique os sistemas que contêm um hub e uma infraestrutura secundária (consulte no Infrastructure Manager; confirme verificando em **Painel de Controle->Adicionar ou Remover Programas** no sistema cliente).

   Observação: a atualização de hubs secundários pode ser necessária somente se duas ou mais versões anteriores forem atualizadas. Consulte a seção Verificação da instalação ou atualização com êxito (na página 22) para versões do hub e de componentes incluídos nesta release, e compare aos hubs secundários instalados atualmente.

2. Salve uma cópia do arquivo hub.cfg na pasta Nimsoft\hub no sistema. Os parâmetros ideais de tempo limite para o hub atualizado são definidos durante a atualização, substituindo configurações de tempo limite existentes. A Nimsoft recomenda executar o hub atualizado com estes valores ideais para obter um desempenho aprimorado. No entanto, se deseja reverter para as configurações antigas de tempo limite por qualquer motivo, é importante manter um backup do antigo arquivo de configuração do hub.
3. No computador cliente, vá até a página do NMS na web (http://<servername_or_IP_address>:8080).
4. Na página web exibida, escolha o link **Robô do Windows, Hub, Servidor de distribuição,** para atualizar o hub e a infraestrutura do Nimsoft nesse computador.
5. Siga os prompts para concluir a instalação.
6. Repita esse procedimento para outras atualizações de hub.

Atualizar as filas do hub para a detecção

- Após uma atualização, certifique-se de que as informações da detecção de dispositivos (a partir de todos os probes distribuídos envolvidos na detecção automatizada) podem acessar o discovery_server. Isto requer:
  a. A criação de uma fila de anexos para o assunto do **probe_discovery** em todos os hubs secundários que hospedam o discovery_agent, o vmware ou o cm_data_import.
  b. A configuração de uma fila de obtenção com o assunto **probe_discovery** em cada hub, com exceção daqueles na parte inferior da hierarquia de hubs.

Consulte o *Guia do Usuário de Detecção* para obter todo o procedimento sobre como configurar as filas do probe_discovery.

Observação: se todos os componentes de detecção estiverem localizados sob o hub principal, essa comunicação será feita automaticamente, e nenhuma configuração manual de filas será necessária.

Atualizar robôs

Use um ou mais dos seguintes procedimentos.

Windows, método 1

1. Inicie o Gerenciador de infraestrutura no servidor atualizado (ou outro hub com um arquivo morto atualizado). No arquivo morto, localize o pacote **robot_update**.
2. Arraste e solte esse pacote do arquivo morto no ícone do robô que deseja atualizar.

Windows, método 2

1. Identifique outros sistemas que contêm um robô do Nimsoft (visualize com o Gerenciador de infraestrutura, confirme no **Painel de Controle->Adicionar ou Remover** Programas no próprio sistema cliente).
2. No computador cliente, vá até a página do NMS na web (http://<nomedoservidor_ou_endereço_IP_do_servidor>:8080).
3. Escolha o link **Robô do Windows** para instalar o robô do Nimsoft nesse computador.
4. Repita esse procedimento para outras atualizações de robô.

Linux ou Solaris

1. Semelhante ao procedimento para o sistema Windows, descrito acima, solte o pacote **robot_update** de um arquivo morto atualizado no ícone do robô que deseja atualizar.
2. Repita o procedimento para outras atualizações de robô.

Atualizações de robô com implantação em massa

Você pode criar um grupo ou grupos de robôs fora do hub no Infrastructure Manager e, em seguida, implantá-los em massa.

Robôs do hub

Atualize os robôs do hub individualmente, soltando **robot_update** em cada ícone de robô.

Verificação de instalação ou atualização bem-sucedida

Após a instalação, a Nimsoft recomenda verificar a saída do processo de instalação com atenção para detectar quaisquer falhas. Três indicativos de sucesso:

- É possível ver o **Nimsoft Server 7.0** na página web do NMS.
- Você tem as versões atuais de todos os componentes na janela principal do Infrastructure Manager e para as interfaces de usuário (selecione **Ajuda > Sobre** para verificar a versão).
- O novo probe mpse é exibido no Infrastructure Manager e no Console de administração.

Observação: estas tabelas listam os números de versão dos probes fornecidos com o NMS 7.0. Ocasionalmente, a Nimsoft fornece versões mais recentes de alguns probes entre as releases dos pacotes do servidor. As atualizações mais recentes de probes são exibidas no site de suporte da Nimsoft http://support.nimsoft.com http://support.nimsoft.com (nas páginas **Download** e **Arquivo morto**) à medida que ficam disponíveis.

Importante: a operação normal da execução do programa de instalação da Nimsoft, durante uma atualização, é substituir componentes e probes atualmente instalados. Em alguns casos, quando probes de "correção" ou versões especiais/atualizadas de componentes tiverem sido instalados anteriormente para solucionar problemas ou oferecer suporte a requisitos personalizados, a atualização poderá resultar em downgrades de componente. Se isso acontecer, as versões de probe e componentes necessários poderão ser restaurados localizando-os no NM Server Archive e instalando-os em vez do que foi fornecido pela atualização.

Interfaces do usuário	Versão 7.0	Release anterior
Infrastructure Manager	4.08	4.07
Console de administração	7.00	6.50
Dr. Nimbus	1.5.3	1.5.3
Componentes de back-end	**Versão 7.0**	**Release anterior**
alarm_enrichment	4.20	4.20
audit	1.22	1.22
automated_deployment_engine	1.23	1.21
baseline_engine	1.0	1.0
cm_data_import	7.00	6.50
controller	7.00	5.70
distsrv	5.30	5.30

hdb	7.00	5.70
hub	7.00	5.82
spooler	7.00	5.70
NAS	4.20	4.20
robot_update	7.00	5.70
nis_server	3.00	2.72
nimldr	3.57	3.57
data_engine	7.91	7.91
fault_correlation_engine	1.65	1.65
ppm	2.12	2.00
qos_engine	2.67	2.67
qos_processor	1.20	1.20
relationship_services	1.69	1.68
service_host	1.03	1.02
sla_engine	3.60	3.59
Componentes da detecção	**Versão 7.0**	**Release anterior**
ace (versão de várias plataformas)	3.00	2.72
assetmgmt	1.24	1.24
cisco Monitor	3.35	3.32
cm_data_import	7.00	6.50
cdm	4.73	4.70
discovery_agent	7.00	6.50
discovery_server	7.00	6.50
interface_traffic	5.33	5.23
net_connect	2.94	2.90
rsp	3.05	2.92
topology_agent	1.68	1.68

Capítulo 5: Problemas conhecidos

As seções a seguir descrevem os problemas conhecidos e as soluções alternativas em alguns casos.

Desempenho, estabilidade e escalabilidade

ADE (Automated Deployment Engine - Mecanismo de Implantação Automatizada)

A distribuição do robô ADE para destinos do Windows às vezes falha ao ativar os probes hdb e spooler.

Para resolver esse problema, vá para a máquina afetada e execute uma **validação de segurança** nos probes afetados (hdb e spooler).

Reinicialização lenta do discovery_server no MySQL

Quando o Servidor de detecção é iniciado, ele executa um script para verificar/criar tabelas no banco de dados do NIS. Na versão 5.5 do MySQL existe um erro (consulte http://bugs.mysql.com/bug.php?id=63144 e http://dev.mysql.com/doc/relnotes/mysql/5.6/en/news-5-6-13.html) que faz com que a execução desse script seja lenta.

A atualização do MySQL para a versão 5.6.13 ou posterior resolve esse problema.

Ao usar o fluxo 5.5 do MySQL, a solução de contorno é desativar dashboard_engine e encerrar quaisquer consultas pendentes durante a reinicialização do servidor de detecção. Isso possibilitará que o script de criação de detecção prossiga.

Red Hat Enterprise Linux (RHEL)

Os processos do Nimsoft no RHEL 6.1 x86-64 consumem mais memória do que em outras plataformas Linux.

- **Sistemas RHEL v6 de 64 bits**

  Os processos podem utilizar até três vezes a quantidade de memória virtual e residente por processo, em comparação às releases anteriores do RHEL ou a outros sistemas operacionais.

- **Sistemas RHEL v6 de 32 bits**

  Os processos podem utilizar várias vezes mais memória virtual, mas a memória residente por processo é basicamente equivalente.

Facilidade

- **O erro nametoip pode ser exibido**

  Ao atualizar para o NMS 6.0, você pode ver **nametoip** listado como um erro fatal no **ace.log** e no **nis_server.log**. Ele pode ser ignorado. O controlador observa que o ACE encontrou esse erro e reinicia automaticamente o ACE, o que corrige o erro.

- **Ocorrências de permissão no Windows 2008**

  Privilégios de gravação são necessários para gravar na pasta Arquivos de programas do Nimsoft. Se você efetuar logon como um usuário sem privilégios de administrador, após a instalação, você deverá definir manualmente esses privilégios de gravação.

- **A comunicação com o robô pela rede falha devido ao arquivo /etc/hosts inválido**

  Apenas sistemas que não sejam o Windows

  Certifique-se de que o arquivo **/etc/hosts** em qualquer sistema que não seja o Windows hospedando um robô, hub, servidor ou instância UMP do Nimsoft contém uma entrada válida para o computador local. Esse deve ser um par totalmente qualificado de nome do host e endereço IP. Se apenas loopback for definido (por exemplo, localhost 127.0.0.1), o probe do controlador nesse computador não terá conhecimento do seu próprio endereço IP, resultando em uma falha na comunicação de rede.

- **Ativando a detecção e a configuração de um probe interface_traffic existente no servidor**

  A função de detecção do Nimsoft ativa automaticamente a criptografia de sequências de caracteres da comunidade no arquivo de configuração do probe no computador da detecção. Antes de ativar a função de detecção, ative a criptografia no probe de tráfego da interface. Caso isso não seja feito, as configurações existentes param de funcionar devido às sequências de caracteres da comunidade inválidas. Os probes Interface_traffic em outros robôs não são afetados.

- **A instalação silenciosa requer um valor DB_PORT se você usar portas dinâmicas**

  Se estiver instalando com as instâncias nomeadas do MS SQL Server ou com o SQL Server Express e estiver usando portas dinâmicas, você não poderá usar o número de porta padrão (1433), pois isso impedirá que data_engine se conecte ao banco de dados.

  Data_engine ficará verde no Infrastructure Manager (porque está em execução), mas a falta de conexão fará com que a fila aumente continuamente.

  Se a porta padrão tiver sido usada:

  1. No Infrastructure Manager, abra a GUI de configuração do probe data_engine, clicando duas vezes no objeto data_engine.
  2. Na guia Banco de dados, exclua a vírgula e o número da porta (**,1433**) anexados ao nome do servidor do banco de dados.
  3. Especifique a porta correta e, em seguida, reinicie o probe.

- **Correlação de falhas é afetado pela configuração de encaminhamento de alarmes do hub e pela replicação de alarme do NAS**

  Para que o aplicativo Correlação de falhas forneça resultados precisos, certifique-se de que os alarmes e as mensagens de interface_poller dos hubs nas áreas aplicáveis da sua topologia de rede estão sendo encaminhados para o hub em que o FCE (Fault Correlation Engine - Mecanismo de Correlação de Falhas) está em execução. Você deve usar as filas do hub que incluem os assuntos **alarme** e **interface_poller** para encaminhar as mensagens que o FCE exige. Use as filas POST ou GET se desejar enviar ou receber mensagens de um hub para o outro.

  Importante: não ative a replicação de alarme do NAS ou o encaminhamento de alarmes ao usar o FCE, pois isso fará com que os alarmes sejam processados duas vezes e gerará resultados imprevisíveis.

- **Os usuários do MySQL devem desativar o probe qos_processor antes da instalação/atualização do UMP**

  Quando o UMP estiver instalado, o processador de QoS poderá ser reativado.

- **Alguns probes talvez não sejam iniciados após a instalação**

  Alguns probes podem não ser iniciados após a instalação do NMS, devido à ausência de recursos do sistema disponíveis.

  Para corrigir esse problema, edite a chave de registro HKEY_LOCAL_MACHINE\System \CurrentControlSet \Control \Session Manager\SubSystems\Windows:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,512,Windows=On SubSystemType=Windows
ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off
MaxRequestThreads=16
```

  Altere o valor 512 (em texto em **negrito** no exemplo acima) para **1024**.

  Para obter mais informações, consulte o artigo em http://support.microsoft.com/kb/184802 http://support.microsoft.com/kb/184802.

- **Os probes do UMP precisam ser reinicializados após a atualização para o NMS 6.0**

  Se você tiver o UMP instalado, reinicie os probes **wasp** e **dashboard_engine** para evitar quaisquer ocorrências durante o logon no UMP após a atualização do NMS.

- **Os probes não são ativados após a instalação do servidor do Nimsoft**

  Vários componentes são distribuídos e configurados durante a instalação do NMS. Em sistemas mais lentos, alguns probes podem não ser iniciados após a instalação. Isso pode ser detectado no Infrastructure Manager e geralmente é corrigido por meio da ativação manual do probe.

- **Os usuários do Oracle precisam adicionar uma chave ao probe dashboard_engine**

  Durante a instalação do NMS, o programa de instalação tenta configurar a conexão com o banco de dado Oracle.

  Observação: quando for solicitado que você digite um nome de serviço, digite primeiro o SID para o espaço de tabela que planeja usar. Se o sistema informar que não pode se conectar ao banco de dados usando o SID, digite um nome de serviço.

  Se você tiver usado um nome de serviço em vez de um SID, ao final da instalação do UMP você poderá ver uma mensagem de erro listando os probes (que exigem conexão com o banco de dados) cuja inicialização falhou. Se isso ocorrer, adicione uma **Chave** e um **Valor** ao probe dashboard_engine. Isso irá reparar a conexão com o banco de dados do dashboard_engine e permitir a inicialização de quaisquer probes que dependam dela.

Siga estas etapas:

1. Abra o Infrastructure Manager e localize o probe dashboard_engine sob o nó **Serviço**.
2. No dashboard_engine, clique Shift + botão direito do mouse na lista de probes à direita para abrir a caixa de diálogo **Raw Configure**.
3. Abra a pasta **Dados** e adicione a **Chave** e o **Valor** a seguir.

   Chave: jdbc_url_template

   Valor: jdbc:oracle:thin:{1}/{2}@{0}:{7}:{your_SID}
4. Aplique a nova chave e valor e reinicie o dashboard_engine.

- **Computadores com AIX não são encontrados pela detecção usando SNMP**

  Ao usar SNMP, determinados tipos de computadores com AIX podem não ser encontrados porque o formato no campo de descrição do computador não pode ser lido. (O AIX envia dados binários como descrição pela API de SNMP que o NMS usa.)

- **Problemas no banco de dados SQLite no Solaris 9**

  Você pode ver os erros SQLITE_BUSY ou SQLITE_CORRUPT no discovery_agent.log. Esses erros podem ser ignorados, contanto que sejam esporádicos e o **discovery_agent** pareça funcionar (por exemplo, continua a detectar novos sistemas e atualiza o “tempo de atividade” dos sistemas monitorados).

  Uma ocorrência mais séria é quando o discovery_agent para de funcionar e você vê o seguinte erro durante a inicialização:

```
Failed to initialize the database file, correct the error and start the probe again.
```

  Para corrigir o problema:

  1. Desative o discovery_agent.
  2. Exclua os arquivos **.db3** e **.dbz** do diretório do discovery_agent:

     <Nimsoft_install_folder>\probes\service\discovery_agent*.db3

     <Nimsoft_install_folder>\probes\service\discovery_agent*.dbz
  3. Ative o discovery_agent.

- **O agente de detecção não funciona em um robô passivo**

  A Nimsoft está investigando uma possível correção em uma futura release.

Uma mensagem "Certificado SSL não confiável" ao iniciar o Console de administração

Se você configurar o probe service_host para usar comunicação segura entre o servidor e o navegador que está executando o Console de administração, um certificado autoassinado será criado pelo processo do service_host. Ao iniciar o Console de administração como autônomo (não em um portlet do UMP), talvez você veja um erro 501 informando que o certificado não é confiável. Pode-se optar por ignorar essa mensagem e continuar, ou configurar o navegador para se confiar no certificado. Como alternativa, em alguns casos, poderá ser vantajoso provisionar um certificado de uma Autoridade de Certificação (CA) e instalá-lo no NMS. Se o certificado for de uma fonte comercial conhecida, os navegadores poderão reconhecê-lo sem a necessidade de nenhuma configuração adicional.

Um certificado SSL será codificado para um nome de host específico (foo.bar.com) ou para um intervalo de hosts em um domínio (*.bar.com). Se for necessário entrar em contato com o servidor por endereço IP (por exemplo, https://1.2.3.4:8443), o navegador exibirá um aviso de certificado não confiável. Entrar em contato com o servidor por meio de https://foo.bar.com:8443 não recebe esse aviso porque o URL usado corresponde ao nome do host no certificado SSL. Especifique o nome do host no campo **Nome DNS** na GUI de configuração do service_host. Consulte a ajuda online do service_host sob o tópico intitulado "Detalhes da configuração" -- para obter mais informações de referência.

Para obter informações sobre o procedimento para configurar certificados SSL para o Console de administração no service_host, consulte a seção "Gerenciando a segurança" na documentação online do Console de administração, disponível também na biblioteca de documentação do Nimsoft.

Console de administração: não foi possível aceitar o certificado SSL no UMP

Problema:

Esse problema ocorre quando Console de administração está configurado para usar um certificado SSL autoassinado para a comunicação com o processo do service_host no NMS.

Ao iniciar o Console de administração como um portlet no UMP pela primeira vez, você receberá um erro 501 informando que o certificado SSL autoassinado não é confiável, mas não será fornecido nenhum meio para aceitar o certificado e continuar. Isso ocorre devido a uma limitação de como alguns navegadores lidam com os certificados SSL dentro de um iframe seguro.

Solução:

Para solucionar esse problema, abra primeiro o Console de administração autônomo em um navegador da web (https://<NMS_host>:8443), onde você poderá ver a mesma mensagem de segurança e poderá aceitar o certificado. Em seguida, o Console de administração será aberto no UMP (no mesmo navegador, no mesmo endereço IP) sem esse problema.

Como alternativa, na caixa de diálogo de erro no UMP que o navegador mostra (o certificado não é confiável. Não foi possível estabelecer a comunicação com o <URL>), copie o URL específico e cole em outra janela ou guia do navegador (no mesmo navegador que está executando o UMP) e aceite o certificado. Retorne ao UMP e recarregue a página para limpar o erro 50.

O Console de administração não funciona após a reinicialização do hub

Problema:

Normalmente, após a reinicialização de um hub que hospeda o probe service_host, você descobrirá que não é possível estabelecer a conexão com o Console de administração. Solucione o problema verificando o arquivo service_host.log. Procure uma mensagem recente que inclua o texto **falha ao pesquisar o data_engine no hub**. Esse problema geralmente só é visto após uma reinicialização do hub, e não é visto em um sistema que foi executado de modo contínuo.

Solução:

Reinicie o probe service_host. Quando o service_host, o probe recipiente para a funcionalidade do Console de administração, perder o contato com o data_engine, a reinicialização do service_host encaminha a ocorrência como uma solução alternativa.

O link do Gerenciador de NiS no Infrastructure Manager não funciona

Sintoma

Quando eu clico no link do Gerenciador de NiS no Infrastructure Manager, recebo uma mensagem de erro: "Erro ao executar o comando: C:\Arquivos de Programas (x86)\Nimsoft\bin\NiSmgr.exe."

Causa

O aplicativo do Gerenciador de NIS foi removido da versão mais recente do NMS. Para configurar componentes de detecção, visite o Assistente de detecção localizado no Portlet do USM.

ADE: use a autenticação de senha de SSH wtih OpenSUSE12.x

Por padrão, o OpenSUSE desativa a autenticação de senha do SSH. Se desejar usar a autenticação de senha de SSH, siga estas etapas:

1. Abra o arquivo /etc/sshd_config com um editor.
2. Localize a entrada "PasswordAuthentication no" e altere para "PasswordAuthentication yes"
3. Salve o arquivo e feche o editor.

Se você não usar a autenticação de senha, você deve usar a autenticação de chave pública de RSA. Consulte a seção Valores de parâmetro para host-profiles.xml no Apêndice A: Implantação em massa com mecanismo de implantação automatizada no Guia de Instalação do NMS. A documentação está disponível na biblioteca de documentação do Nimsoft.

O probe PPM não é suportado no AIX

O probe PPM não será executado em hubs do AIX. Para configurar robôs e probes em hubs do AIX, use a configuração simples com base na web ou o Gerenciador de infraestrutura herdado.

Ocorrências de permissão no Windows 2008

Privilégios de gravação são necessários para gravar na pasta Arquivos de programas do Nimsoft. Se você efetuar logon como um usuário sem privilégios de administrador, após a instalação, você deverá definir manualmente esses privilégios de gravação.

É necessário um único fuso horário

Para que o carimbo de data e hora dos dados funcione corretamente em uma implantação distribuída do Nimsoft, o servidor do NMS, o servidor do UMP e do banco de dados devem ser todos definidos com o mesmo fuso horário, independentemente das localidades geográficas dos servidores.

Encaminhamento de alarme do hub e replicação de alarme do NAS afeta a correlação de falha

Problema:

A correlação de falhas é afetada pela configuração de encaminhamento de alarmes do hub e pela replicação de alarme do NAS.

Solução:

Para que o aplicativo Correlação de falhas forneça resultados precisos, certifique-se de que os alarmes e as mensagens de interface_poller dos hubs nas áreas aplicáveis da sua topologia de rede estão sendo encaminhados para o hub onde o probe FCE (Fault Correlation Engine - Mecanismo de Correlação de Falhas) está em execução. Você deve usar as filas do hub que incluem os assuntos alarme e interface_poller para encaminhar as mensagens que o FCE exige. Use as filas POST ou GET se desejar enviar ou receber mensagens de um hub para o outro.

Importante: não permita a replicação de alarme do NAS ou encaminhamento ao usar FCE. Isso faz com que os alarmes sejam processados duas vezes e produz resultados imprevisíveis.

UNIX: a comunicação do robô falha devido /etc/hosts inválidos

Problema:

Em sistemas que não são Windows, a comunicação do robô pela rede falha devido ao arquivo /etc/hosts inválido.

Solução:

Certifique-se de que o arquivo **/etc/hosts** em qualquer sistema que não seja o Windows hospedando um robô, hub, servidor ou instância UMP contendo uma entrada válida para o computador local. Esse deve ser um par totalmente qualificado de nome do host e endereço IP. Se apenas loopback for definido (por exemplo, localhost 127.0.0.1), o probe do controlador nesse computador não terá conhecimento do seu próprio endereço IP, resultando em uma falha na comunicação de rede.

Não foi possível encontrar um dispositivo no USM pelo endereço IP

Como parte dos aprimoramentos do servidor de detecção e do agente de detecção 7.0, um dispositivo com vários endereços IP agora é exibido como um único dispositivo no USM (Unified Service Manager - Gerenciador de Serviços Unificados) e não como vários dispositivos distintos por endereço IP. Se não for possível localizar um dispositivo no USM por um endereço IP, tente pesquisar pelo nome.

Localização

Sequências de caracteres traduzidas são erros no arquivo de log de instalação (iaoutput.txt).

Instalação

Falha na instalação devido à versão do Java JRE

O programa de instalação de pré-verificação pode indicar um problema com o Java Runtime Environment (JRE) se ele encontrar a versão 29 ou 30 do Java 6 (JRE 1.6.29 ou 1.6.30).

Observação: há um problema conhecido com o JRE 1.6.29 e o 1.6.30 (Java 6 versões 29 e 30) ao trabalhar com o MS SQL Server (consulte: http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7105007) http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7105007.

A Nimsoft recomenda que você instale a atualização mais recente do JRE SE 6 ou SE 7, dependendo de qual versão você esteja usando. Para o JRE 6, ele é atualmente o JRE 1.6u43 (Java 6 atualização 43). Para JRE 7, ele é 1.7u17 (Java 7 atualização 17).

Observação: a instalação no Windows Server 2012 exige o JRE 1.6u38 / 1.7u6 ou posterior para que a plataforma do sistema operacional seja detectada de forma adequada.

Solaris apenas:

A pré-validação do programa de instalação sinaliza quando um JRE de 32 bits é instalado em uma plataforma Solaris de 64 bits. Com o Solaris, o uso do JRE de 64 bits como referência JRE para o NMS é obrigatório.

- Certifique-se de que possui um JRE de 64 bits instalado antes de executar o programa de instalação.
- Além disso, verifique o PATH para ver se (1) um JRE de 64 bits está listado e (2) listado antes de qualquer JRE de 32 bits.

Observação: o Solaris é diferente de outras plataformas uma vez que o JRE de 64 bits está localizado um diretório mais abaixo.

Em sistemas AMD64, o caminho completo para o diretório JRE de 64 bits é normalmente:

```
/usr/java/jre/bin/amd64
```

Em sistemas SPARC, o caminho completo para o diretório JRE de 64 bits é normalmente:

```
/usr/java/jre/bin/sparcv9
```

- Verifique se o PATH inclui o diretório JRE de 64 bits e, em seguida, execute novamente o programa de instalação.

O agente de detecção e outros probes emitem alarme de ocorrência na atualização

Sintoma

O agente de detecção e alguns outros probes podem enviar um único alarme informativo ao atualizar para a versão mais recente do NMS. Esse alarme é benigno e pode ser ignorado com segurança.

Causa

O Servidor de detecção cria uma fila de barramentos dos quais esses outros probes dependem. A fila pode não estar totalmente operacional quando esses probes são ativados, o que faz com que o alarme informativo seja enviado. A fila será ativada em um curto período de tempo.

A instalação do NMS falha no CentOS, OpenSuse e RHEL

Sintoma

A instalação do servidor do NM falha no CentOS, no OpenSUSE versão 12 ou no RHEL de 32 bits.

Causa

O Mecanismo de dados requer libstdc++.so.5 { libstdc++-3.3.4-11.x86_64.rpm }

A instalação do lib compatível resolve o problema.

Emita este comando:

```
yum install compat-libstdc++-33
```

Recomendável: implantar o PPM para cada hub no seu domínio

Para usar a configuração com base na web para qualquer hub remoto ou robôs/probes nesse hub, o PPM precisa ser distribuído para esse hub.A Nimsoft recomenda que o PPM seja implantado em cada hub dentro de seu domínio.

Alguns probes talvez não sejam iniciados após a instalação

- **Instalação do NMS no Windows**

  Após instalação do NMS em sistemas Windows, alguns probes podem não iniciar devido à falta de recursos disponíveis do sistema.

  Para corrigir esse problema, edite a chave de registro HKEY_LOCAL_MACHINE\System \CurrentControlSet \Control \Session Manager\SubSystems\Windows:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512,Windows=On
SubSystemType=Windows ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
```

  Altere o valor 512 (em texto em **negrito** no exemplo acima) para **1024**.

  Para obter mais informações, consulte o artigo em http://support.microsoft.com/kb/184802.

- **Instalação do NMS em todas as plataformas**

  Vários componentes são distribuídos e configurados durante a instalação do NMS. Em sistemas mais lentos, alguns probes podem não ser iniciados após a instalação. Isso pode ser detectado no Gerenciador de infraestrutura ou no Console de administração e é corrigido por meio da ativação manual do probe.

- Atualização do **NMS em todas as plataformas**

  Se você atualizar para o NMS e possui o UMP instalado, reinicie os probes **wasp** e **dashboard_engine** para evitar qualquer problema ao efetuar o logon no UMP após a atualização.

Instalação do UMP no MySQL

Os usuários do MySQL devem desativar o probe QoS_processor antes de instalar ou atualizar o UMP no NMS 6.50. Quando o UMP estiver instalado, o processador de QoS poderá ser reativado.

ADE: Instalando o robô em Debian v6

Por padrão, o Debian v6 usa o endereço 127.0.1.1 como o endereço de resolução de nomes. Quando um robô é implantado em um sistema Debian 6 usando ADE, após a reinicialização do sistema o robô tentará vincular-se a 127.0.1.1, pois é o endereço disponível. Use a seguinte solução alternativa para evitar a contenção de 127.0.1.1 no sistema Debian 6:

1. Ao instalar o robô *manualmente* ou com o *ADE*, é necessário ir até o sistema de destino após a operação e adicionar a linha a seguir ao arquivo robot.cfg:

   ```
   robotip = ip_address
   ```

   em que **ip_address** é o endereço IP a que o robô deve se vincular no computador de destino.

2. Ao implantar uma caixa de Debian 6.0.5 usando *XML*, é necessário definir a opção **<robotip>ip_address</robotip>**, em que **ip_address** é o endereço a que o robô deve se vincular no computador de destino.

Autenticação LDAP: usuários do grupo do administrador que não seja do domínio não podem efetuar logon no servidor do NM

Um usuário LDAP não poderá efetuar logon no servidor do NMS exceto se o usuário do Active Directory for um integrante do grupo do administrador do domínio LDAP. A diretiva de grupo do LDAP no NMS não importa.

Instalação silenciosa com SQL Server: valor DB_PORT obrigatório com portas dinâmicas

Se estiver instalando com as instâncias nomeadas do MS SQL Server ou com o SQL Server Express e estiver usando portas dinâmicas, você não poderá usar o número de porta padrão (1433), pois isso impedirá que data_engine se conecte ao banco de dados.

Data_engine ficará verde no Infrastructure Manager (porque está em execução), mas a falta de conexão fará com que a fila aumente continuamente.

Se a porta padrão tiver sido usada:

1. No Infrastructure Manager, abra a GUI de configuração do probe data_engine, clicando duas vezes no objeto data_engine.
2. Na guia **Banco de dados**, exclua a vírgula e o número da porta (**,1433**) anexados ao nome do servidor do banco de dados.
3. Especifique a porta correta e, em seguida, reinicie o probe.

Solaris: Falha na instalação reduz o espaço de troca disponível

Se a instalação do NMS for interrompida ou falhar por qualquer razão, os arquivos de instalação (/tmp/install.*) não são excluídos. Como a troca no Solaris inclui o diretório /tmp, a Nimsoft recomenda excluir manualmente esses arquivos antes de executar o programa de instalação novamente.

Linux com o MySQL: o acesso foi negado para o usuário root

Problema:

Ao tentar instalar o NMS com um banco de dados MySQL, você poderá ver o erro a seguir (ou seu equivalente) depois de digitar as informações do servidor de banco de dados:

```
ERROR 1045 (28000): Access denied for user 'root'@'<your Nimsoft hostname>' (using password: YES)
```

Isto ocorre porque os privilégios remotos não foram estabelecidos ou porque a senha identificada para os sistemas remotos não está de acordo com aquela definida no servidor de banco de dados localmente.

Solução:

Execute estas etapas:

1. Efetue logon no banco de dados MySQL localmente (ou seja, no servidor que hospeda o MySQL).
2. Para configurar o acesso de qualquer host, execute:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql> GRANT TRIGGER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> GRANT SUPER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES
```

Para definir o acesso de um determinado host, execute estes comandos, substituindo *HostX* pelo nome do seu host:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root' AND Host = 'HostX';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'HostX' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql> GRANT TRIGGER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> GRANT SUPER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES;
```

Windows: erro de IP inválido ao instalar o infrastructure

Problema:

Quando você executa o **NimBUS Infrastructure.exe** para instalar o robô do Windows, hub, servidor de distribuição, é possível ver a seguinte mensagem de erro:

```
IP da linha de comando não é válido: 127.0.0.1
```

Solução:

Esse erro é benigno e pode ser ignorado com segurança. Basta clicar em OK e continuar.

Capítulo 6: Defeitos corrigidos

Esta seção descreve os defeitos (organizados por categoria) que foram corrigidos no NMS 7.0.

Desempenho, estabilidade e escalabilidade

- US8238 a detecção não identifica vários IP de dispositivos na rede (por exemplo, roteadores ou comutadores) como um dispositivo.
- US19631 / SF00098482 os dispositivos são exibidos várias vezes no USM.
- US19630 / SF00098484 alguns dispositivos listam duas origens quando os nomes são correspondentes.
- SF00104689 origens duplicadas em sistemas monitorados remotamente.
- DE23018 CM_Computer_System: o nimbus_type é alterado para 0 quando o robô é movido para outro hub.
- DE25575 o discovery_server falha ao inserir registros quando o tamanho do campo de origem é excedido.
- DE 22432 os novos hubs secundários/remotos demoram para aparecer no Infrastructure Manager/Console de administração.

Facilidade

- DE15765 instalação de agrupamento do Microsoft Server - as chaves de licença padrão de 30 dias são geradas com um endereço IP virtual e os probes são iniciados com um IP local/físico.
- DE22425 alterar o nível de um alarme usando alarm_enrichment.
- DE22438 alarme de tamanho da fila inoperável.
- DE23018 quando um robô se move de um hub para outro, o nmbus_type é alterado para um valor de 0.